REMARKS

Status of Claims:

Claims 1-22 are present for examination.

Allowable Subject Matter:

Applicant expresses appreciation to the Examiner for the indication that claims 7, 8, 10, 11, 13, 14, 16, and 17 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejection:

Claims 1-6, 9, 12, 15, and 18-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ateniese et al. "Some Open Issues and New Directions in Group Signatures" (hereinafter Ateniese) in view of Jakobsson (U.S. Patent Number 6,317,833 B1).

With respect to claims 1-6, 9, 12, 15, and 18-22, as amended, the rejection is respectfully traversed.

Independent claim 1, as amended, recites a system comprising:

> "a participant subsystem that is authorized to anonymously participate in a plurality of sessions using secret information provided by a manager subsystem, all of said secret information being transmitted to the participant subsystem prior to participation in a first of said plurality of sessions, said secret information enabling participation in each of the plurality of sessions; and
>
> a reception subsystem;
>
> wherein the participant subsystem comprises:
>
> an anonymous signing section for authorizing particular individual data using the secret information depending on session-related information to produce anonymous participation data with an anonymous signature;
>
> wherein the reception subsystem comprises:

an anonymous signature determining section for determining whether received data is said anonymous participation data with said anonymous signature; and

a sender match determining section for determining whether anonymous signatures of two **different** pieces of anonymous participation data **representing two different contents of individual data** that are received in a same session of said plurality of sessions are signed by an **identical** participant subsystem; and

wherein **participation** by said participant subsystem in a plurality of different sessions is **concealed** from said reception subsystem." (Emphasis Added).

A system including the above-quoted features has at least the advantages that: (i) a sender match determining section of a reception subsystem can determine whether anonymous signatures of two **different** pieces of anonymous participation data representing **two different contents** of individual data that are received in a same session of a plurality of sessions are signed by an **identical** participant subsystem; and (ii) **participation** by a participant subsystem in a plurality of different sessions is **concealed** from the reception subsystem. (Specification; page 3, lines 17-23; page 4, lines 21-26; page 5, line 21 to page 6, line 21; page 7, lines 1-5; page 22, lines 1-18; page 31, lines 5-15).

Neither Ateniese nor Jakobsson, alone or in combination, disclose or suggest a system including the above quoted features. In the discussion that follows, each of Ateniese and Jakobsson will be examined, and then the combination of Ateniese and Jakobsson will be examined.

a. Ateniese:

The group signature scheme of Ateniese does not allow for determining whether anonymous signatures of two **different** pieces of anonymous participation data that represent **two different contents** of individual data that are received in a same session of a plurality of sessions are signed by an **identical** participant subsystem.

Ateniese examines the use of group signatures for various applications. (Ateniese; abstract). Ateniese begins by reciting the properties of group signatures, and notes that a group signature scheme must satisfy the security property of **unlinkability**, which means that deciding whether two **different** signatures were computed by the same group member is **computationally hard**. (Ateniese; section 1, paragraph 1; section 2, paragraph 3, reference "Unlinkability"). Ateniese then later examines the special case of sub-group signatures (**SGS**). (Ateniese; sections 9-10).

As defined in Ateniese, a SGS is an operation with respect to a **single** message m. (Ateniese; section 9, paragraph 1). The central goal of SGS is to demonstrate that a subset of a certain size of group members has signed the **same** message m. (Ateniese; section 9, paragraph 6). For example, a petition may be circulated among members of a certain group, and a number of members "i" may sign the petition and then publicly announce that "i" members stand behind it, while any insider or outsider is able to verify that "i" distinct members have indeed signed the petition. (Ateniese; section 9, paragraph 5).

Ateniese allows for weakening the unlinkability property with respect to SGS in order to achieve compositional integrity in which a verifier can be assured that all signatures comprising a SGS have been generated by distinct signers. (Ateniese; section 9, paragraphs 7 and 8). Thus, a VERIFY procedure for a SGS in Ateniese allows for a verifier to check if the **same** message m has been signed more than once by a given signer. (Ateniese; section 10, paragraph 5).

However, a system as recited in claim 1 including the above-quoted features allows for a reception subsystem to determine whether anonymous signatures of two **different** pieces of anonymous participation data representing **two different contents of individual data** that are received in a same session of a plurality of sessions are signed by an identical participant system. It is important to recognize that the SGS of Ateniese **only** allows for checking for a redundant signature by a given signer if the message m signed by both signatures is the **same** message m. (Ateniese; section 10). This is because a SGS can be defined **only** for a **single** message m. This is seen by the "petition" example in Ateniese where **only** a **single** petition can be signed with one SGS. (Ateniese; section 9, paragraphs 1 and 5).

If two **different** messages were to be signed with the method of Ateniese, either a regular group signature would be required or two different SGS's would be required. While Ateniese allows for weakening the unlinkability property within a **single** SGS, Ateniese states that, "we emphasize that this should be done **only** for SGS; i.e., the structure of other types of group signatures (regular, multi-group) must remain **unchanged**." (Ateniese; section 9, paragraph 8) (Emphasis Added). Thus, in Ateniese, the unlinkability property remains for regular group signatures, so if **two different messages** were signed with regular group signatures, there would be **no** way to check if an identical participant subsystem signed both. Also, if two different SGS-s are used for two **different** messages in the method of Ateniese, it would be computationally difficult to decide whether subgroups that produced the signatures have any member is common. (Ateniese; section 10.1, lemma 2). This is because, in the method of Ateniese, there is a property of unlinkability among different SGS-s. (Ateniese; section 10.1).

Therefore, while Ateniese may allow for determining if the **same** message m has been signed twice by an identical signer, the method of Ateniese does **not** allow for determining if two **different** messages have been signed by an identical signer.

b. Jakobsson:

The mix-based election scheme of Jakobsson does **not** allow for **participation** by a participant subsystem in a plurality of different sessions to be **concealed** from a reception subsystem.

In the system of Jakobsson, all eligible voters have a pair of secret and public keys associated with them. (Jakobsson; column 2, lines 49-50). Each pair is different, and only the voter in question knows his/her secret key. (Jakobsson; column 2, lines 50-52). The public keys in the system of Jakobsson are either recorded in a list of all eligible voters or are certified by a Certifying Authority. (Jakobsson; column 2, lines 52-53).

When tallying votes in the system of Jakobsson, the talliers verify that each particular voter's **public key** was **only used to sign one message**. (Jakobsson; column 3, lines 36-44). Such a system in Jakobsson allows for detecting whether a voter has voted more than once in a single election even if the voter submits different votes in the election. However, because each voter in Jakobsson must have a different public key from other voters and the voter uses the same public key in each election, **participation** by a voter in a plurality of different elections **cannot** be **concealed** in the system of Jakobsson. This is because the talliers will notice that the same public key has been used to sign messages in two different elections and, thus, will **know** that a **same voter** has **participated** in both elections. (Jakobsson; column 3, lines 34-51).

Therefore, the mix-based election scheme of Jakobsson does **not** allow for **participation** by a voter in a plurality of different elections to be **concealed** from talliers.

c. Combination of Ateniese and Jakobsson:

Even if the mix-based election scheme of Jakobsson were combined with the group signature scheme of Ateniese, the combined scheme would still **not** allow for **both**: (i) determining whether anonymous signatures of two different pieces of anonymous participation data representing two different contents of individual data that are received in a same session of a plurality of sessions are signed by an identical participant subsystem; and (ii) **participation** by a participant subsystem in a plurality of different sessions to be **concealed** from a reception subsystem.

In a combined system of Ateniese and Jakobsson, voters would each be assigned a pair of secret and public keys, where each pair would be different. (Jakobsson; column 2, lines 49-53). Then, talliers in the combined system would be able to verify that each particular voter's public key was only used to sign one message in a given election. (Jakobsson; column 3, lines 34-51). However, since the same public keys would be used in different elections, if a voter voted in two different elections, then the **participation** of the voter in the two different elections would be **known** to the talliers, because they would **know** that a same public key has been used the two elections.

As a consequence, even if Jakobsson were combined with Ateniese, the combined scheme would **not** allow for **participation** by a voter/signer in a plurality of different elections to be **concealed** from a tallier/verifier.

Moreover, even if a different secret key and public key were used by a voter for each election, which is not disclosed by Jakobsson, the resulting system would still not meet the limitations of the present claim, because the present claim requires that the same secret information enables participation in each of the plurality of sessions.

Therefore, independent claim 1, as amended, is neither disclosed nor suggested by the Ateniese and Jakobsson references and, hence, is believed to be allowable. The Patent Office has not made out a *prima facie* case of obviousness under 35 U.S.C. 103.

Independent claim 18, as amended, recites an anonymous participation authority management method with features similar to features of a system of independent claim 1 and, thus, is believed to be allowable for at least the same reasons that independent claim 1 is believed to be allowable.

The dependent claims are deemed allowable for at least the same reasons indicated above with regard to the independent claims from which they depend.

Conclusion:

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 50-0872. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 50-0872.

If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 50-0872.

Respectfully submitted,

Date December 16, 2005

By

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (310) 975-7965
Facsimile: (310) 557-8475

Justin M. Sobaje
Attorney for Applicant
Registration No. 56,252